Switches: The Basics

Cabrillo College

CIS 83 (CCNA 3)

Rick Graziani

Cabrillo College

Fall 2006

Note to instructors

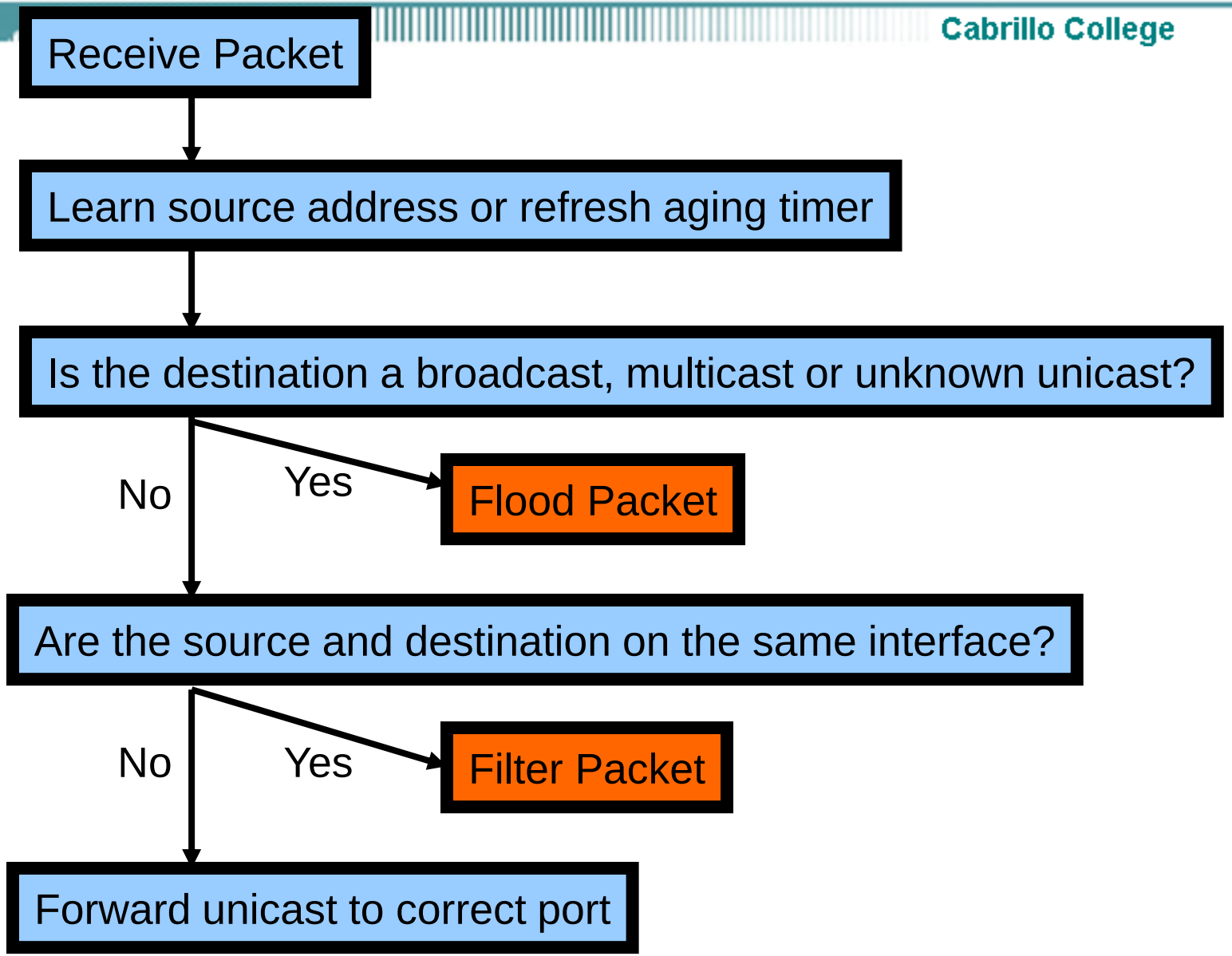
- If you have downloaded this presentation from the Cisco Networking Academy Community FTP Center, this may not be my latest version of this PowerPoint.
- For the latest PowerPoints for all my CCNA, CCNP, and Wireless classes, please go to my web site:

  http://www.cabrillo.edu/~rgraziani/

  - The username is *cisco* and the password is *perlman* for all of my materials.
- If you have any questions on any of my materials or the curriculum, please feel free to email me at graziani@cabrillo.edu (I really don't mind helping.) Also, if you run across any typos or errors in my presentations, please let me know.
- I will add "(Updated – *date*)" next to each presentation on my web site that has been updated since these have been uploaded to the FTP center.

Thanks! Rick

Transparent Bridge Process - Jeff Doyle

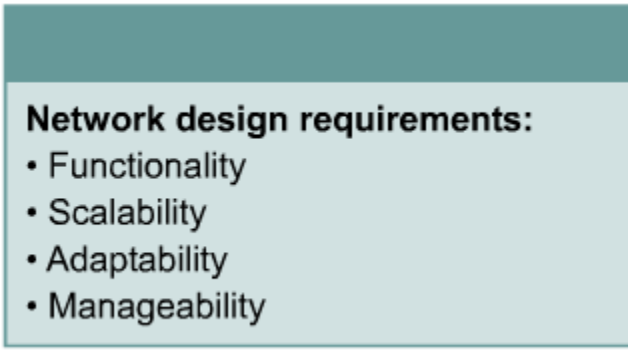


Switch Process – Another Look

For every frame that enters a switch…

- Learning Stage (Building/Updating of SAT/MAC table)
  - Examines **Source MAC Address**:
    - If **Source MAC Address** is in the SAT/MAC table, update 5 minute timer
    - If **Source MAC Address** is NOT in the SAT/MAC table, add Source MAC Address and incoming port number to SAT/MAC table
- Forwarding Stage (Flood or Filter)
  - Examines **Destination MAC Address**:
    - If **Destination MAC Address** is in the SAT/MAC table, forward the frame only out that port (**Filter**), unless it is the outgoing port is the same as the incoming port (checks Source MAC Address)
    - If **Destination MAC Address** is NOT in the SAT/MAC table, forward the frame only out all ports except incoming port (**Flood**)

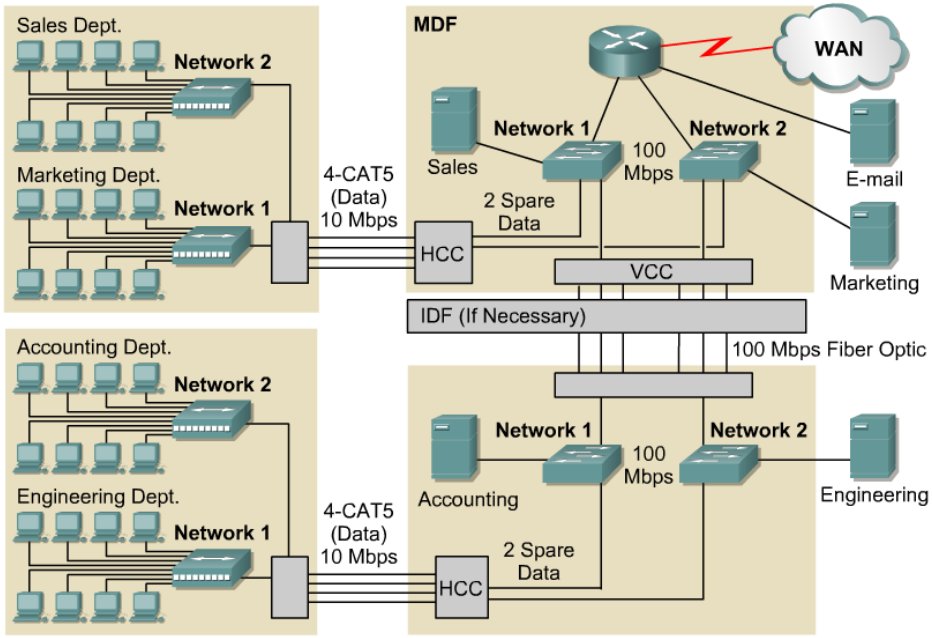
LAN Design Goals



- **Functionality** – The network must work. The network must allow users to meet their job requirements. The network must provide user-to-user and user-to-application connectivity with reasonable speed and reliability.
- **Scalability** – The network must be able to grow. The initial design should grow without any major changes to the overall design.
- **Adaptability** – The network must be designed with a vision toward future technologies. The network should include no element that would limit implementation of new technologies as they become available.
- **Manageability** – The network should be designed to facilitate network monitoring and management to ensure ongoing stability of operation.

LAN design considerations

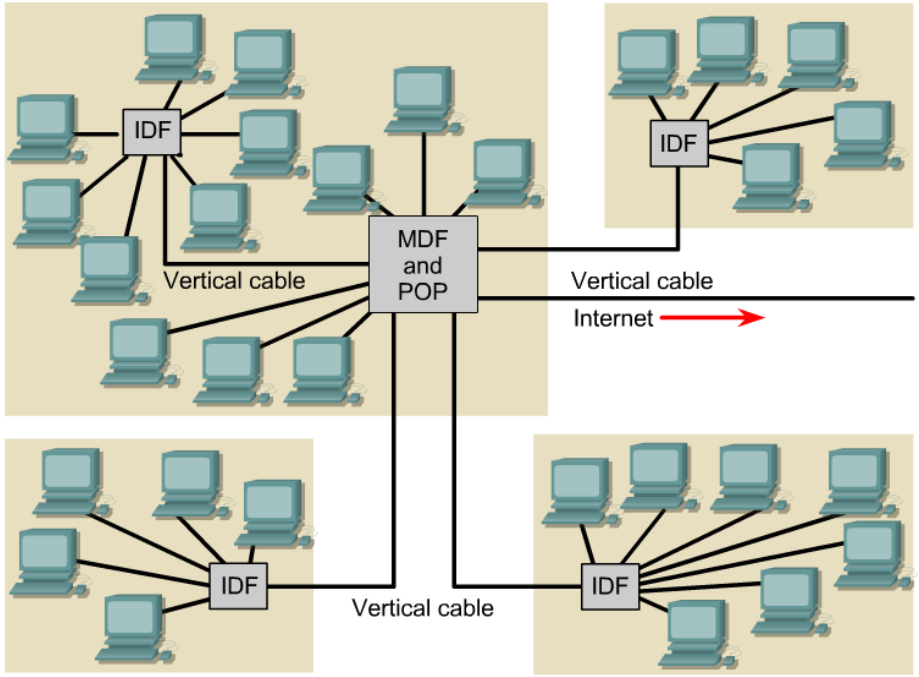
Server Placement



- Servers can be categorized into two distinct classes:
  - **Enterprise servers**
  - **Workgroup servers**
- An **enterprise server** supports all the users on the network by offering services, such as e-mail or Domain Name System (DNS) that everyone in an organization would need because it is a centralized function.
- A **workgroup server** supports a specific set of users, offering services such as word processing and file sharing.
  - Other examples might include applications that are specific to a group of users.

LAN design considerations

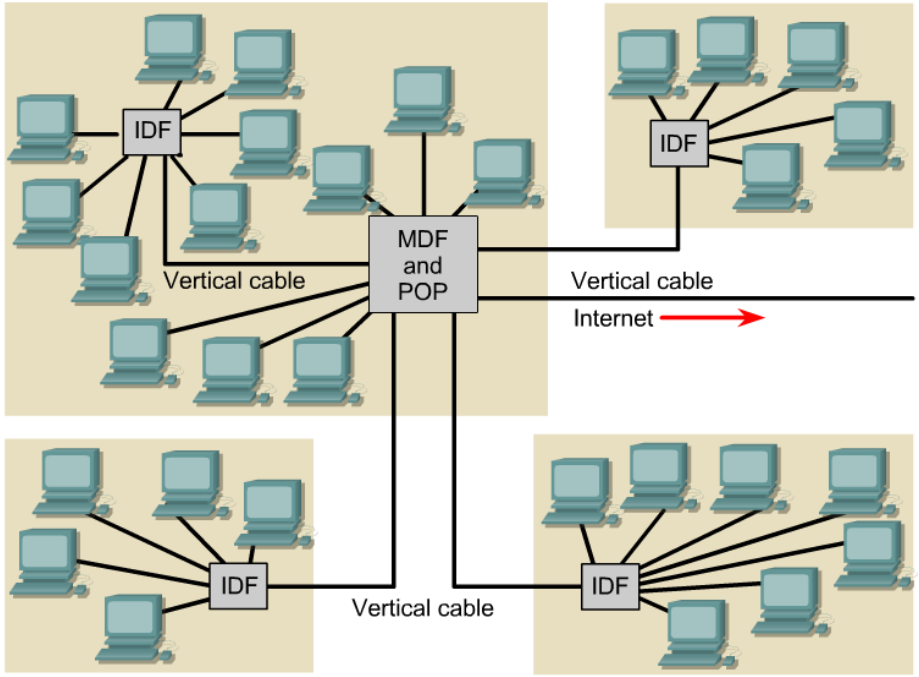
Server Placement



- **Enterprise servers** should be placed in the **main distribution facility (MDF).**
  - Traffic to the enterprise servers travels only to the MDF and is not transmitted across other networks. (Not necessarily. If you have a "routed core" it will travel across other networks.)

LAN design considerations

Server Placement

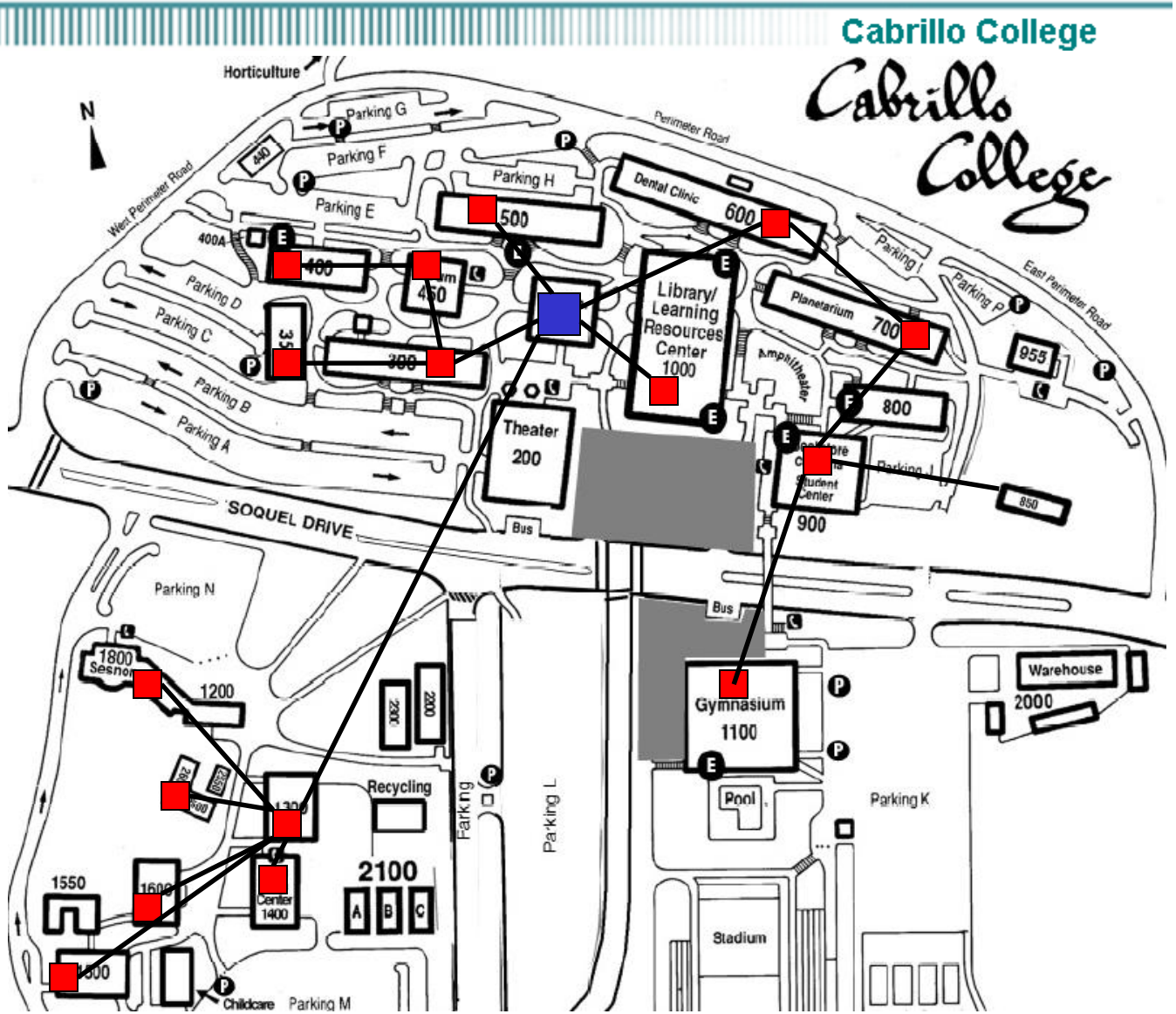


- Ideally, **workgroup servers** should be placed in the **intermediate distribution facilities (IDFs)** closest to the users accessing the applications on these servers.
  - By placing workgroup servers close to the users, traffic only has to travel the network infrastructure to an IDF, and does not affect other users on that network segment.
  - Layer 2 LAN switches located in the MDF and IDFs should have 100 Mbps or more allocated to these servers.

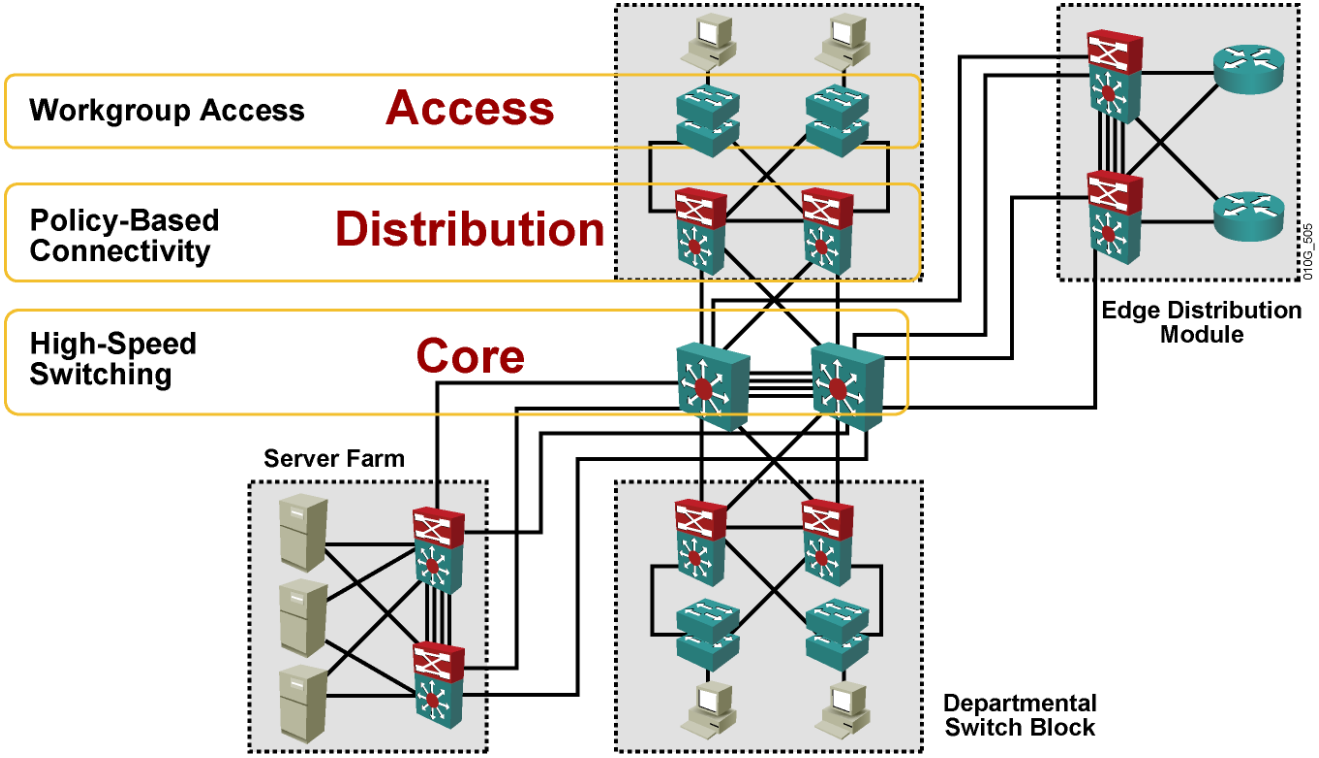
Cabrillo College – MDF/IDF Map

MDF

IDF



Switched LANs, access layer overview



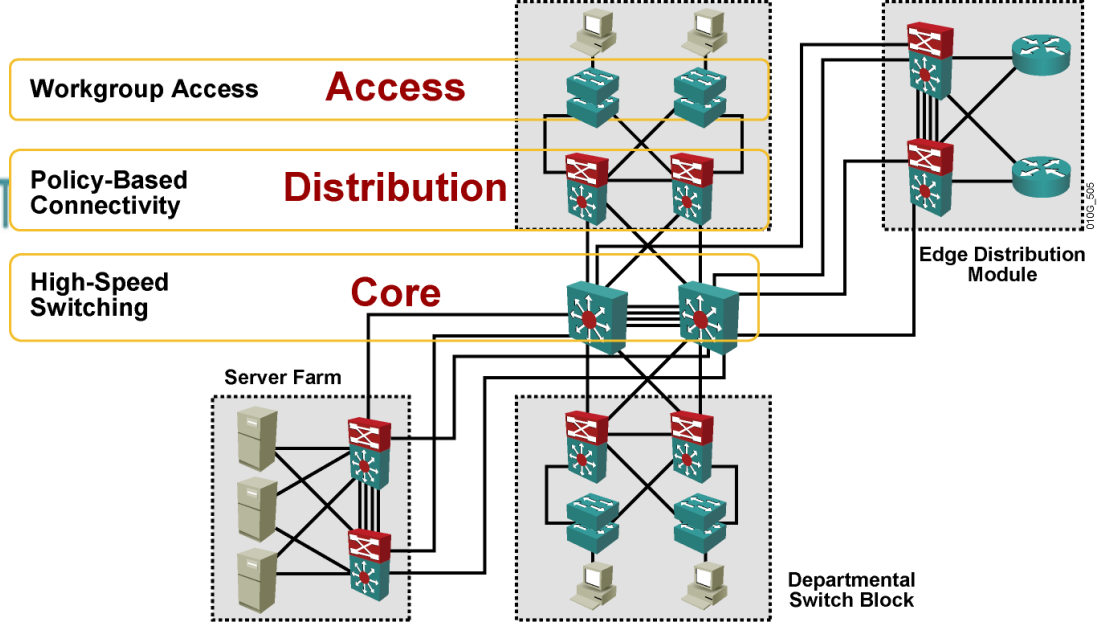
The hierarchical design model includes the following three layers:

- The **access layer** provides users in workgroups access to the network.
- The **distribution layer** provides policy-based connectivity.
- The **core layer** provides optimal transport between sites.
  - The core layer is often referred to as the backbone.

Access layer switches

- Access layer switches operate at **Layer 2** of the OSI model and provide services such as VLAN membership.
- The main purpose of an access layer switch is to allow end users into the network.
- An access layer switch should provide this functionality with low cost and high port density.
  - Catalyst 1900 series
  - Catalyst 2820 series
  - Catalyst 2950 series
  - Catalyst 4000 series
  - Catalyst 5000 series

Distribution Layer



- The purpose of this layer is to **provide a boundary definition** in which packet manipulation can take place.
- Networks are **segmented into broadcast domains** by this layer.
- **Policies** can be applied and access control lists can filter packets.
- The distribution layer also **prevents problems from affecting the core layer**.
- Switches in this layer operate at **Layer 2 and Layer 3**.
- The distribution layer includes several functions such as the following:
  - Aggregation of the wiring closet connections
  - Broadcast/multicast domain definition
  - Virtual LAN (VLAN) routing
  - Any media transitions that need to occur
  - Security

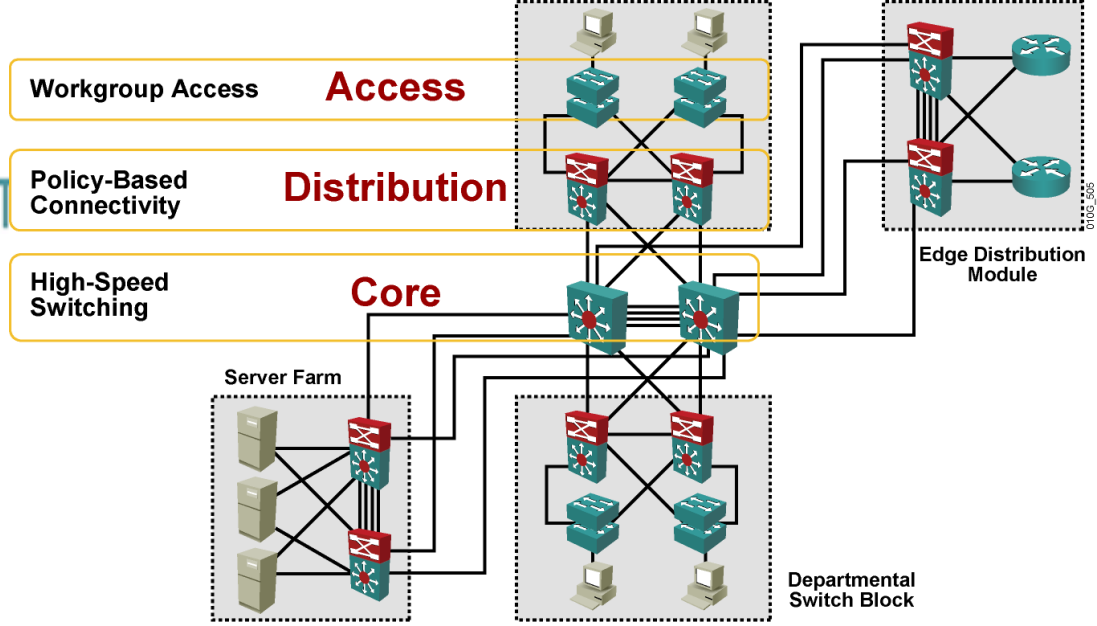
Distribution layer switches

2926G

6500

- Distribution layer switches are the aggregation points for multiple access layer switches.
- The switch must be able to accommodate the total amount of traffic from the access layer devices.
- The distribution layer combines VLAN traffic and is a focal point for policy decisions about traffic flow.
- For these reasons distribution layer switches operate at both Layer 2 and Layer 3.
- The following Cisco switches are suitable for the distribution layer:
  - Catalyst 2926G
  - Catalyst 5000 family
  - Catalyst 6000 family

Core Layer



- The core layer is a **high-speed switching** backbone.
- If they do not have an associated router module, an external router is used for the Layer 3 function.
- This layer of the network design should **not perform any packet manipulation.**
- Packet manipulation, such as access list filtering, would slow down the switching of packets.
- Providing a core infrastructure with redundant alternate paths gives stability to the network in the event of a single device failure.

Core Layer Switches

Lightstream 1010

8540

- In a network design, the core layer can be a routed, or Layer 3, core.
- Core layer switches are designed to provide efficient Layer 3 functionality when needed.
- Factors such as need, cost, and performance should be considered before a choice is made.
- The following Cisco switches are suitable for the core layer:
  - Catalyst 6500 series
  - Catalyst 8500 series
  - IGX 8400 series
  - Lightstream 1010

Switch Configuration

Cabrillo College

CIS 83 (CCNA 3)

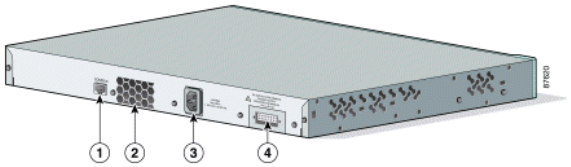
Rick Graziani

Cabrillo College

Fall 2006

Physical startup of the Catalyst switch

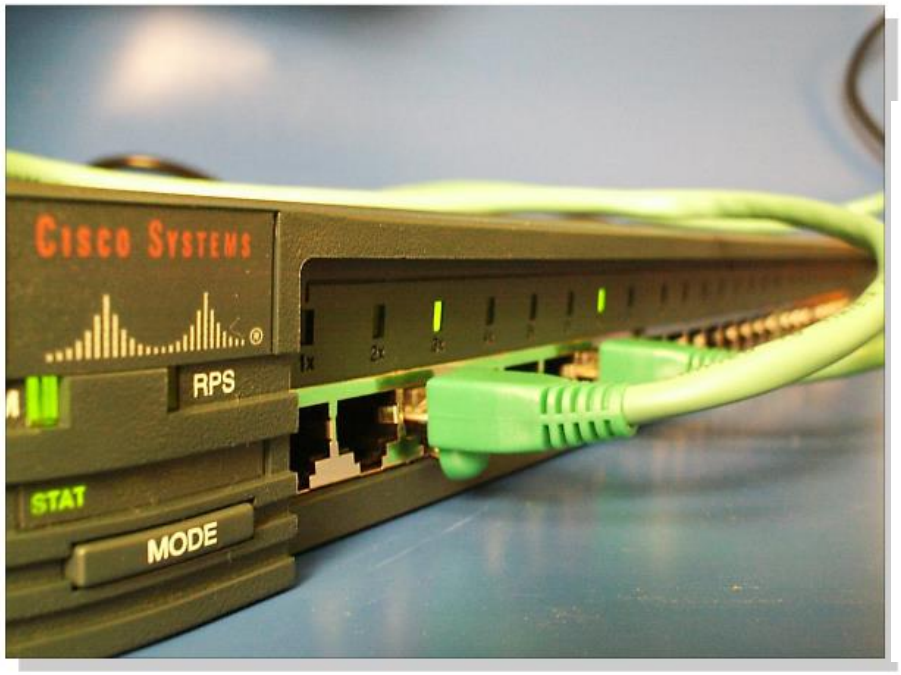
Figure 2-3 Catalyst 2970 Switch Rear Panel

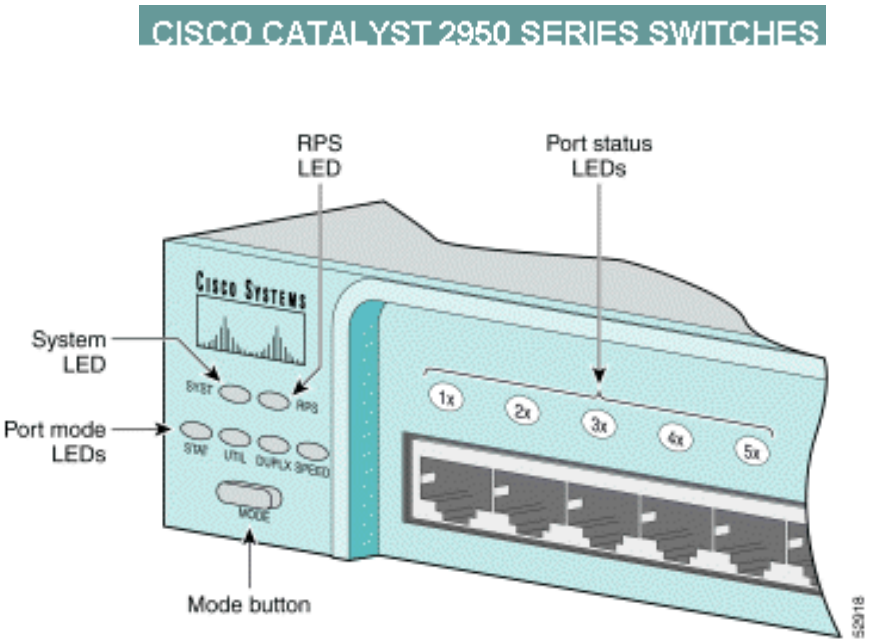


1	RJ-45 console port
2	Fan exhaust
3	AC power connector
4	RPS connector

- Switches are dedicated, specialized computers;
  - Central Processing Unit (CPU)
  - Random Access Memory (RAM)
  - Operating System
- A switch can be managed by connecting to the console port to view and make changes to the configuration.
- Lower model switches typically have no power switch to turn them on and off.
- They simply connect or disconnect from a power source.

Switch LED indicators

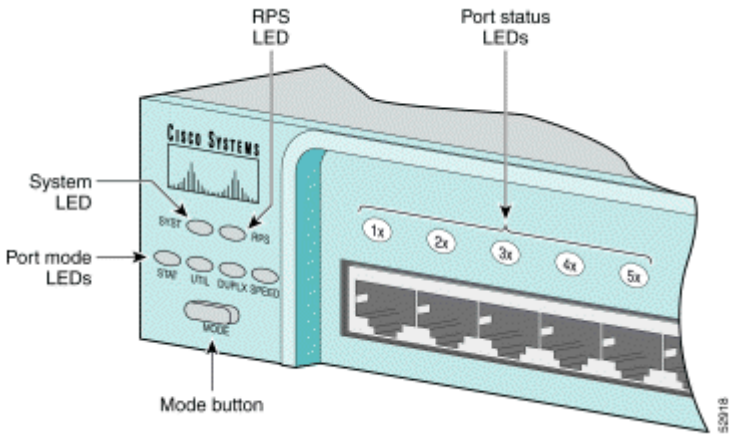


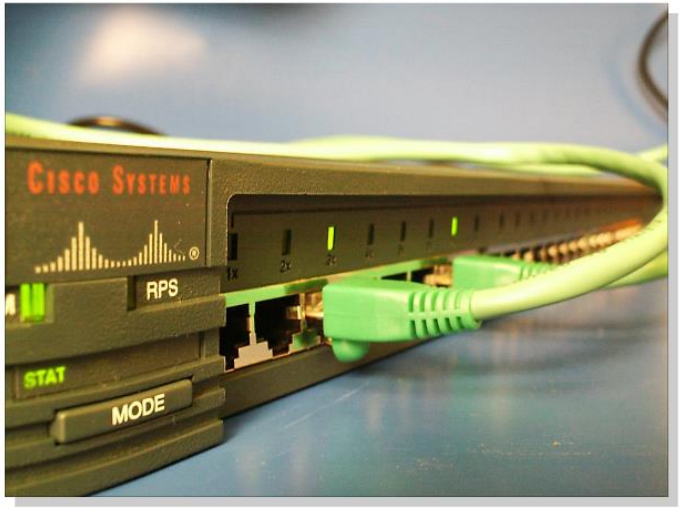


- We will examine LED indicators.
- Note: Many of these are switch specific, although green is usually good.
- LED indicators are only quick view of the status of the switch.
- For a more detailed view, use IOS commands.

Switch LED indicators - 2950

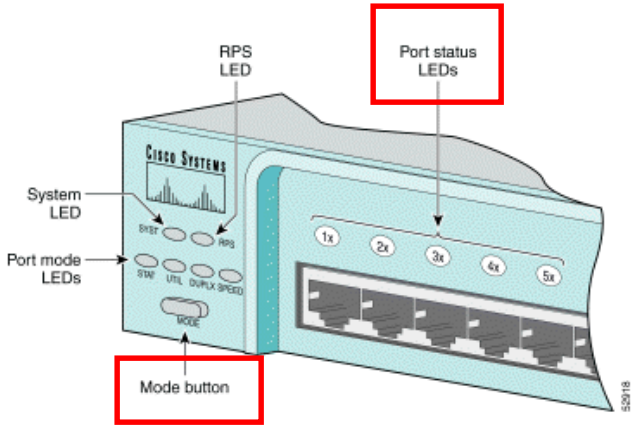
- The front panel of a switch has several lights to help monitor system activity and performance.
- These lights are called light-emitting diodes (LEDs).
- The front of the switch has the following LEDs:
  - **System LED**
    - Whether the system is receiving power and functioning correctly.
  - **Remote Power Supply (RPS) LED**
    - Whether or not the remote power supply is in use
  - **Port Mode LED**
    - Indicates the current state of the Mode button.
    - The modes are used to determine how the Port Status LEDs are interpreted.
  - **Port Status LEDs**
    - Has different meanings, depending on the current value of the Mode LED.

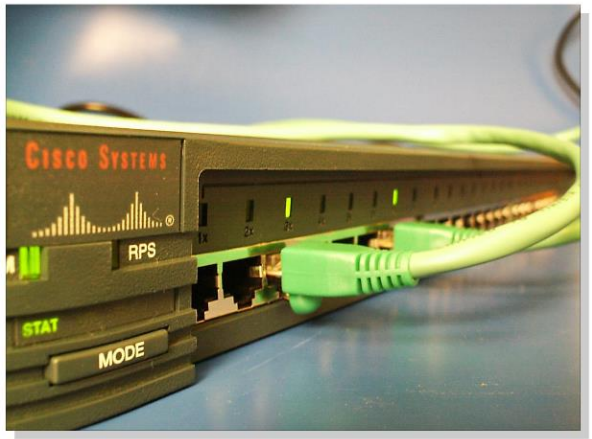




Switch LED indicators: Port Status LED

Mode LED	Color	Description
STAT	Off	No link
	Solid Green	Link operational
	Flashing Green	Port is sending or receiving data
	Alternating green/amber	Link fault
	Solid amber	Port is not forwarding because it was disabled by management or address violation, or blocked by Spanning/Tree Protocol.
UTL	Off	Each LED that is off indicates a reduction by half of the total bandwidth. The LEDs are turned off from right to left. If the right-most LED is off, then the switch is using less than 50% of total bandwidth. If the two right-most LEDs are off, the switch is using less than 25% of total bandwidth.
	Green	If all LEDs are green, the switch is using 50% or more of total bandwidth.
FDUP	Off	Port is operating in half-duplex mode.
	Green	Port is operating in full-duplex mode.
100	Off	Port is operating at 10 Mbps.
	Green	Port is operating at 100 Mbps.



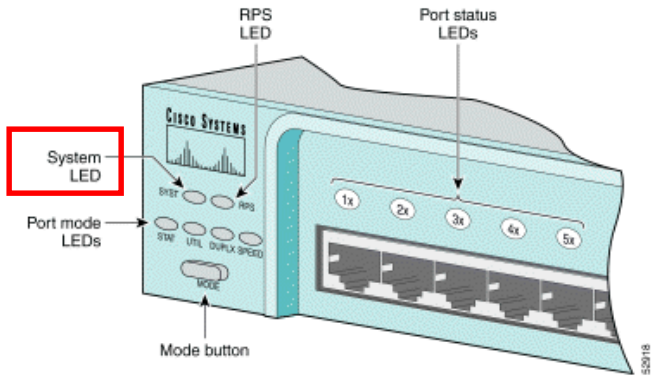


Port LEDs during switch POST – System LED

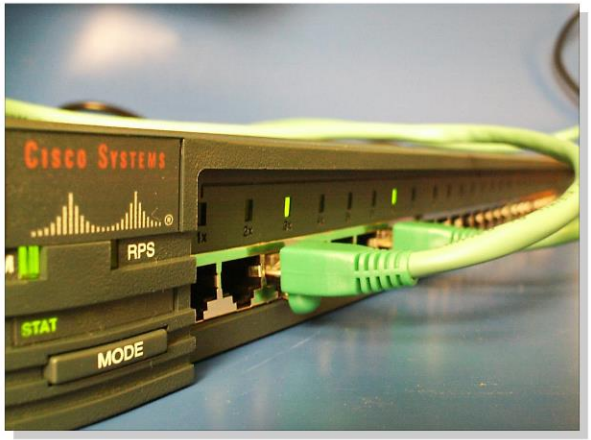
System LED

The System LED indicates the success or failure of POST.

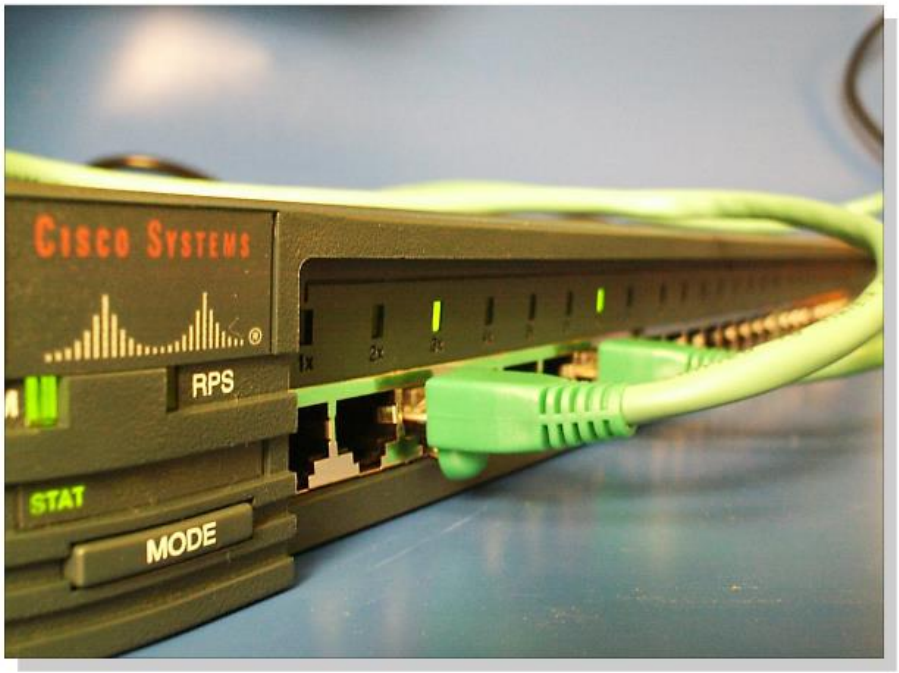
- If the System LED is off but the switch is plugged in, then POST is running.
- If the System LED is green, then POST was successful.
- If the System LED is amber, then POST failed.

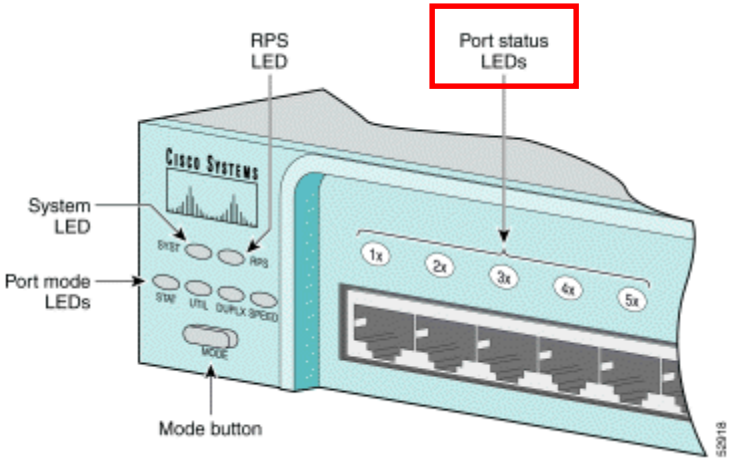


- Once the power cable is connected, the switch initiates a series of tests called the power-on self test (POST).
- If the System LED is **green**, then POST was successful.
- If the System LED is **amber**, then POST failed. POST failure is considered to be a fatal error.



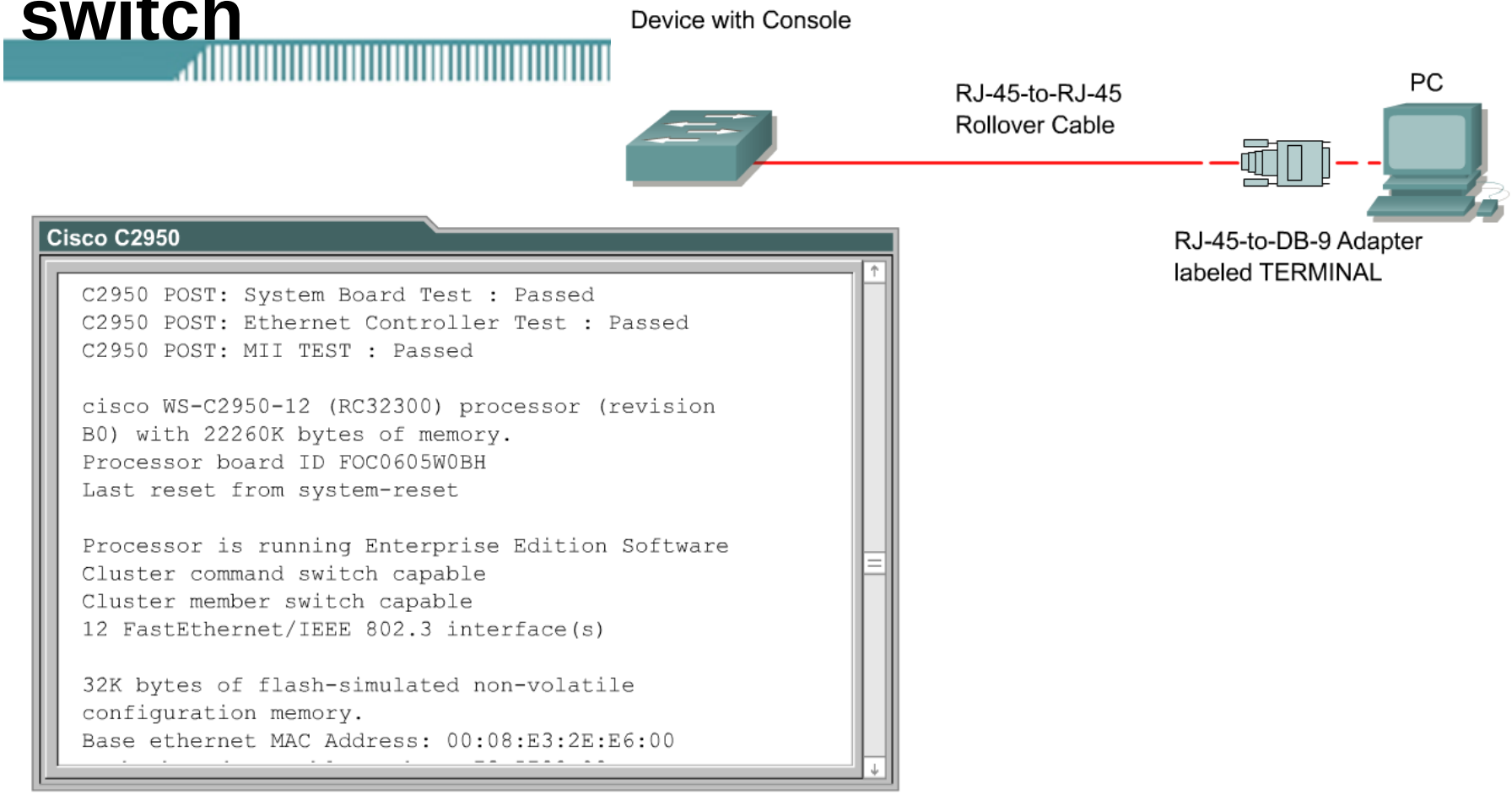
Port LEDs during switch POST – Port Status LED





- The Port Status LEDs also change during switch POST.
- The Port Status LEDs turn **amber** for about 30 seconds as the switch discovers the network topology and searches for loops.
- If the Port Status LEDs turn **green**, the switch has established a link between the port and a target, such as a computer.
- If the Port Status LEDs turn **off**, the switch has determined that nothing is plugged into the port.

Viewing initial bootup output from the switch



- The switch may be configured manually with or without the assistance of the System Configuration dialog.
- The System Configuration dialog on the switch is simpler than that on a router.

Examining help in the switch CLI

Cisco

```
Switch>?

Exec commands:

access-enable    Create a temporary Access-List entry

clear            Reset functions

connect          Open a terminal connection

disable          Turn off privileged commands

disconnect       Disconnect an existing network
                 connection

enable           Turn on privileged commands
```

- The command-line interface (CLI) for Cisco switches is very similar to the CLI for Cisco routers.

Show running-config


```
ALSwitch#show running-config
Building configuration...

Current configuration : 1300 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ALSwitch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
interface FastEthernet0/1
```

show interface


```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is
0008.e32e.e501 (bia 0008.e32.e.e601)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
    reliability 255/25, txlead 1/255, rxlead 1/255
  Encapulation ARPA, Loopback not set
  Keepalive not set
  Auto-duplex, AutoSpeed , 100BaseTX/TX
  ARP type: ARPA, ARP TImeout 04:00:00
  Last Input never, output 00:31:54, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue o/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
```

show vlan


```
Switch#show vlan
VLAN Name                Status  Ports
---- ------------------- ------  -------------------------
1    default             active  Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                 Fa0/9, Fa0/10,Fa0/11,Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type  SAID    MTU   Parent RingNo BridgeNo
---- ----- ------  ----- ------ ------ --------
1    enet  100001  1500  -      -      -
1002 fddi  101002  1500  -      -      -
1003 tr    101003  1500  1005   0      -
1004 fdnet 101004  1500  -      -      1
```

show flash


```
Switch#show flash or Switch#dir flash:
Directory of flash:/

  2  -rwx     1674921   Apr 30 2001 15:09:51  c2950-
c3h2s-mz.120-5.3.WC.1.bin
  3  -rwx         269   Jan 01 1970 00:00:57
env_vars
  4  drwx       10240   Apr 30 2001 15:09:52  html

7741440 bytes total (4780544 bytes free)
```

show version


```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version
12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000

ROM: Bootstrap program is CALHOUN boot loader

Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-
5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with
22260K bytes of memory.
Processor board ID FOC0605W0BH
```

Reset all Switch Configurations & Reload

Catalyst 2950

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload
```

Catalyst 1900

```
Switch#delete nvram
```

The following steps will ensure that a new configuration will completely overwrite any existing configuration:

- Remove any existing VLAN information by deleting the VLAN database file vlan.dat from the flash directory
- Erase the back up configuration file startup-config
- Reload the switch

Security, documentation, and management


```
Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
ALSWitch(config-line)#line vty 0 4
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
```

- The same class rules apply for passwords on switches as they did on routers.
- “cisco” and “class”
- We will not need to configure “enable secret”, console, and vty passwords until the case study.

Set IP Address and Default Gateway


```
ALSwitch(config)#interface VLAN1
ALSwitch(config-if)#ip address 192.168.1.2
255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1
```

- To allow the switch to be accessible by Telnet and other TCP/IP applications, IP addresses and a default gateway should be set.
- By default, VLAN 1 is the management VLAN. (more later)
- In a switch-based network, all internetworking devices should be in the management VLAN.
- This will allow a single management workstation to access, configure, and manage all the internetworking devices.
- The **default gateway** is only for management purposes, not for user Ethernet frames (and packets).
- This is only used if you wanted to telnet from this switch into a device on another network.

Set Port Speed and Duplex Settings


```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

- The Fast Ethernet switch ports default to:
  - auto-speed
  - auto-duplex.
- This allows the interfaces to negotiate these settings.
- When a network administrator needs to ensure an interface has particular speed and duplex values, the values can be set manually.

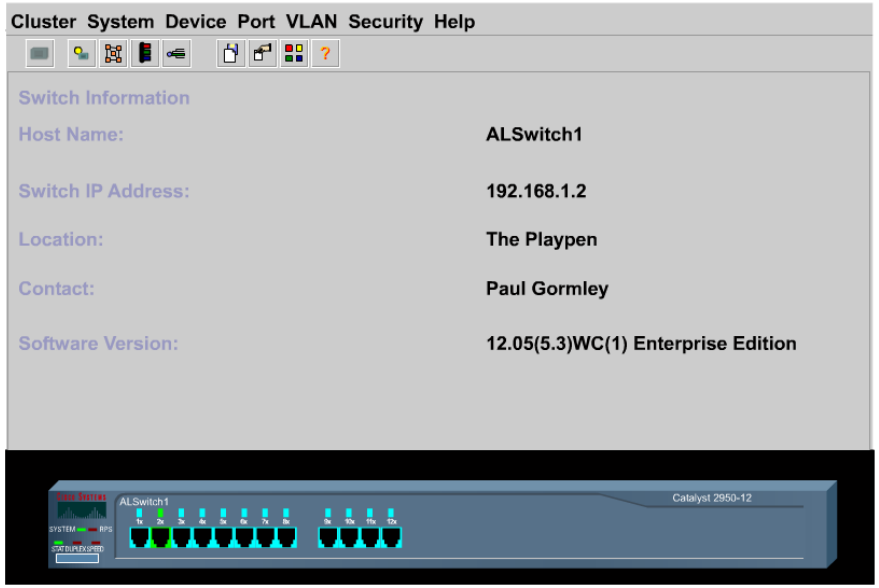
- More later…

HTTP Service and Port


```
Switch#configure terminal
Enter configuration commands, one per line.  End
with CNTL/Z.
Switch(config)#ip http ?
  access-class    Restrict access by access-class
  authentication  Set http authentication method
  path            Set base path for HTML
  port            HTTP port
  server          Enable HTTP server
Switch(config)#ip http server
Switch(config)#ip http port ?
  <0-65535>  HTTP port
Switch(config)#ip http port 80
Switch(config)#
```

- A web browser can access this service using the IP address and port 80, the default port for http.
- The HTTP service can be turned on or off, and the port address for the service can be chosen.

The GUI Interface



Managing the MAC address table


```
Switch#show mac-address-table
Dynamic Address Count:                  2
Secure Address Count:                   0
Static Address (User-defined) Count:    0
System Self Address Count:              13
Total MAC addresses:                    15
Maximum MAC addresses:                  8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination
Port
-------------------  ------------  ----  --------------
0010.7a60.ad7e       Dynamic          1  FastEthernet0/2
00e0.2917.1884       Dynamic          1  FastEthernet0/5
```

- Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port.
- Machines may have been removed from a port, turned off, or moved to another port on the same switch or a different switch.
- This could cause confusion in frame forwarding.
- The MAC address entry is automatically discarded or aged out after **300 seconds**.

Managing the MAC address table


```
Switch#clear mac-address-table
Switch#show mac-address-table
Dynamic Address Count:                    0
Secure Address Count:                     0
Static Address (User-defined) Count:      0
System Self Address Count:                13
Total MAC addresses:                      14
Maximum MAC addresses:                    8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination
Port
-------------------  ------------  ----  --------------
```

- Rather than wait for a dynamic entry to age out, the administrator has the option to use the privileged EXEC command **`clear mac-address-table.`**

Configuring static MAC addresses


```
Switch(config)#mac-address-table ?
  aging-time  Set MAC address table entry maximum
age
  secure      Configure a secure address
  static      Configure a static 802.1d static
address
Switch(config)#mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
Switch(config)#no mac-address-table static
0010.7a60.1884 interface FastEthernet0/5 VLAN1
```

- The reasons for assigning a permanent MAC address to an interface include:
  - The MAC address will not be aged out automatically by the switch.
  - A specific server or user workstation must be attached to the port and the MAC address is known.
  - If the device is moved on the switch, it will not be able to reached.
  - Security is enhanced.
- To set a static MAC address entry for a switch:

`Switch(config)#` **`mac-address-table static`** *<mac-address of host>* **`interface FastEthernet`** *<Ethernet numer>* **`vlan`**

Copying IOS from TFTP Server


```
ALSwitch#copy tftp flash
Address or name of remote host []? 192.168.1.3
Source filename []? c2950-c3h2s-mz.120-5.3.WC.1.bin
Destination filename [c2950-c3h2s-mz.120-5.3.WC.1.bin]? [enter]
%Warning: There is a file already existing with this name

Do you want to over write? [confirm] [enter]
Accessing tftp://192.168.1.3/c2950-c3h2s-mz.120-5.3.WC.1.bin...
Loading c2950-c3h2s-mz.120-5.3.WC.1.bin from 192.168.1.3 (via VLAN1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
[OK - 1674921 bytes]
1674921 bytes copied in 51.732 secs (32841 bytes/sec)
ALSwitch#
```

Erasing and Reloading the Switch

Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]

Switch#erase startup-config


Switch(config)#reload
```

The responding line prompt will be:

```
System configuration has been modified. Save? [yes/no]:
```

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

Port Security

Note: Port Security will be discussed in another presentation.

Switch Configuration

Cabrillo College

CIS 83 (CCNA 3)

Rick Graziani

Cabrillo College

Fall 2006